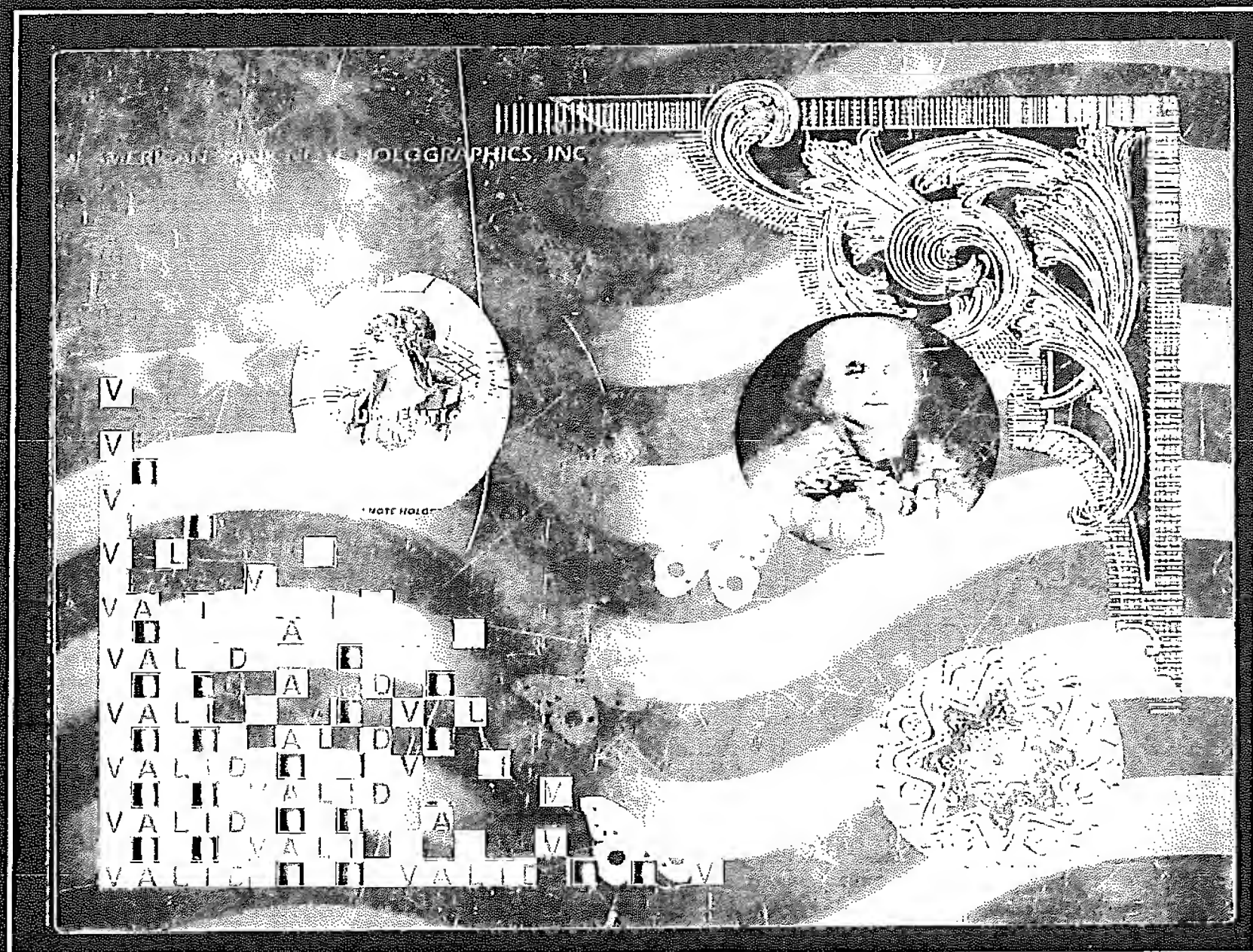
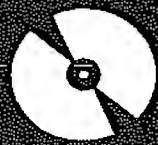


Optical Document Security

THIRD EDITION



Rudolf L. van Renesse



CD-ROM
INCLUDED

Optical Document Security

Third Edition

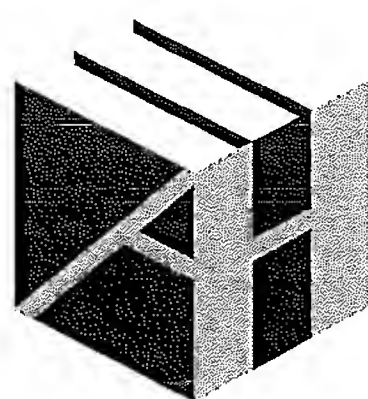
Rudolf L. van Renesse

Arjo Wiggins Security

SAS au capital de 70 000 000 €

Siège social : 117 quai du Président Roosevelt
92442 ISSY-les-MOULINEAUX Cedex
FRANCE

(RCS Nanterre 433 753 258) - Tél. 33 (0)1 41 08 60 00



**ARTECH
HOUSE**

BOSTON | LONDON
artechhouse.com

Library of Congress Cataloguing-in-Publication Data

A catalog record for this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data

van Renesse, Rudolf L.

Optical document security.—3rd ed.—(Artech House optoelectronics library)

1. Counterfeits and counterfeiting—Prevention 2. Identification cards—Forgeries—Prevention 3. Reproduction of money, documents, etc.—Prevention 4. Electronics in crime prevention 5. Legal documents—Design—Security measures

I. Title

364.1'63

ISBN 1-58053-258-6

Cover design by Igor Valdman

Cover hologram by AmericanBank Note Holographics, United States

© 2005 Rudolf L. van Renesse

All rights reserved.

Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 1-58053-258-6

10 9 8 7 6 5 4 3 2 1

Contents

Preface to the Third Edition	<i>xiii</i>
Acknowledgments	<i>xvii</i>

CHAPTER 1

Introduction to Optical Document Security: The Color of Light and Matter	1
1.1 Introduction	1
1.2 The Intrinsic Color of Matter	2
1.2.1 Optically Invariable Matter	2
1.2.2 The Main Optical Phenomena	3
1.3 Color Theory	6
1.3.1 Eye Sensitivity	6
1.3.2 Primary Colors and the Mixing of Colors	8
1.3.3 Complementary Colors	12
1.3.4 Maxwell's Color Triangle	15
1.3.5 The CIE Chromaticity Diagram	16
1.3.6 The Limitation of Subtractive Color Mixing	20
1.3.7 Color Separation and Color Reproduction	22
1.3.8 Uniform Color Space: CIELAB	25
1.3.9 Colorfastness	27
References	29

CHAPTER 2

Introduction to Optical Document Security: The Color of Colorless Matter	31
2.1 Introduction	31
2.2 Metallic Reflection	32
2.3 Light Interference and Diffraction	32
2.3.1 The Interference of Wave Patterns	33
2.3.2 Light Diffraction by Gratings	36
2.3.3 The Recording and Reconstruction of Interference Patterns	40
2.4 Interference Colors: Thin Films	47
2.4.1 The Colors of Single Layer Structures	47
2.4.2 The Colors of Multilayer Structures	54
2.5 Discussion	59
References	60

CHAPTER 3

Substrate-Based Security	63
3.1 Introduction	63
3.2 Paper Substrates	63
3.2.1 Composition	63
3.2.2 Watermarks	64
3.2.3 Chemical Reactants	68
3.2.4 Mechanical Properties: Feel and Sound	70
3.2.5 Fluorescence	71
3.2.6 Size of Valuable Documents	72
3.2.7 Tint and Gloss	72
3.2.8 Security Fibers	73
3.2.9 Planchets	75
3.2.10 Embedded Thread	76
3.2.11 Windowed Thread	78
3.2.12 Perforation	79
3.3 Plastic Substrates	83
3.3.1 Plastic Cards	84
3.3.2 Synthetic Papers	89
References	94

CHAPTER 4

Printing Inks and Printing Techniques	97
4.1 Introduction	97
4.2 Printing Inks	97
4.2.1 Reversible Photosensitivity	97
4.2.2 Thermochromic Inks	102
4.2.3 Metameric Inks	104
4.2.4 Bleed-Through Security Numbering	107
4.2.5 Fugitive Inks, Solvents, and Bleaches	109
4.2.6 Iridescent Inks	111
4.2.7 Magnetic Inks	111
4.2.8 Tagging of Valuable Documents and Products	114
4.3 Printing Techniques	115
4.3.1 Intaglio Printing	115
4.3.2 Letterpress Printing	120
4.3.3 Offset Printing	123
4.3.4 Screen Printing	125
References	126

CHAPTER 5

Printed Security Patterns	129
5.1 Introduction	129
5.2 Classic Images	130
5.2.1 Guilloches	130
5.2.2 Microprinting	131
5.2.3 See-Through Register	133

5.2.4	Engraved Portraits	135
5.2.5	Transitory Images	137
5.3	Digitally Watermarked Images	141
5.3.1	Overt Digital Watermarks	142
5.3.2	Covert Digital Watermarks	142
5.4	Screen-Decoded Images	146
5.4.1	Classification of Screen-Decoded Images	146
5.4.2	Carrier-Screen Images	147
5.4.3	Scrambled Images	161
5.4.4	Hidden Images Versus Scrambled Images	163
5.4.5	Application of Screen-Decoded Images	164
	References	167

CHAPTER 6

	Diffraction-Based Security Features	171
6.1	Optical Variability	171
6.1.1	Noniridescent Optical Variability	171
6.1.2	Iridescent Optically Variable Devices	176
6.2	DOVIDs	177
6.2.1	First-Order DOVIDs—General	177
6.2.2	Laser Transmission Holograms	181
6.2.3	First-Order DOVIDs—3D	183
6.2.4	First-Order DOVIDs—Flat Artwork	189
6.2.5	ZODs	212
6.2.6	Semitransparent Overlays	217
	References	220

CHAPTER 7

	Interference-Based Security Features	223
7.1	Introduction	223
7.1.1	General Properties of ISISs	223
7.1.2	Counterfeiting ISISs	225
7.1.3	Single-Layer Structures	225
7.1.4	Enhanced Pearl Luster Pigments	228
7.2	Multilayer Structures	229
7.2.1	All-Dielectric Thin Films	229
7.2.2	Metal-Dielectric Thin Films	231
7.2.3	Liquid Crystals	237
7.2.4	Polymerized Liquid Crystals	245
7.2.5	Volume-Reflection Holography	250
7.2.6	Lippmann Photography	252
7.2.7	Coextruded Multilayers	255
7.2.8	Combinations of DOVIDs and ISISs	258
7.3	Discussion	259
	References	260

CHAPTER 8

Security Design and Evaluation	265
8.1 Development of a Security Product	265
8.1.1 The Security Policy	266
8.1.2 The Risk Analysis	266
8.1.3 The Program of Requirements	269
8.1.4 The Security Program	273
8.2 The Design Process	274
8.2.1 The Function of the Product	274
8.2.2 The Basic Design Cycle	275
8.2.3 The Characteristics of the Design	277
8.3 Some Ergonomic Considerations	279
8.3.1 The Ergonomic Action Cycle	279
8.3.2 Image Complexity	283
8.3.3 Structure Complexity	285
8.4 Evaluation	287
8.4.1 The Evaluation Process	287
8.4.2 Expertise and Tools	288
8.4.3 Evaluation Standards	290
References	292

CHAPTER 9

An Introduction to Biometrics	295
9.1 Introduction	295
9.1.1 Identity and Personal Document Security	295
9.1.2 Three Basic Identifiers	296
9.1.3 Properties of Identifiers	299
9.2 The Basics of Biometrics	302
9.2.1 The Uniqueness of Biometric Characteristics	302
9.2.2 Biometric Procedures	303
9.2.3 The Accuracy of Biometrics	305
9.2.4 Biometric Functional Rates	308
9.3 A Survey of Biometric Techniques	311
9.3.1 Physical Characteristics	313
9.3.2 Behavioral Characteristics	325
9.4 Biometrics on Public-Scale Identification Documents	328
9.4.1 Scalability of Biometric Trials	328
9.4.2 Sabotage of the Enrollment Procedure	329
9.4.3 Zero-Effort Attack	329
9.4.4 Sabotage by Forced Failure to Verify	330
9.4.5 Sabotage of the Biometric Functionality of the Identification Document	330
9.4.6 Legal Aspects	331
9.5 The Promise of Biometrics	331
References	333

Appendix of Optically Variable Devices (OVDs)	339
A.1 Diffractive Optically Variable Image Devices (DOVIDs)	339
Explanation of Figure A.1	341
A.2 Interference Security Image Structures (ISISs) and Combinations of DOVIDs and ISISs	348
About the Author	353
Index	355

usually takes seconds to minutes but may be accelerated by gently warming the compound or by exposing it to nonactinic visible light. Because of their high reactivity, many photochromic compounds are subject to thermal and photochemical degradation. This reduces their number of possible color conversions, which has limited their usefulness in the past. Modern photochromic security inks reportedly allow an indefinite number of color reversions. Examples are invisible to blue, yellow to green, orange to gray, and red to purple. The usual printing techniques are dry offset and letterpress. An example of the effect is given in Figure CD4.1.

An interesting application of photochromic inks is its use as a copy-revealing feature. The original contains a design in purple. This color is readily converted under the intense illumination of the photocopier, resulting in a yellow design on the photocopy [2]. Photochromic effects can be used for write-once-read-many (WORM) data storage to create optical memory in secure documents [3]. Reference is also made to Section 9.4.4 of [4] for further details on photochromic effects.

4.2.1.2 Luminescence

The collective term for the emission of light by substances that are relatively cool is luminescence (*cold light*). It is a reversible process that includes phenomena like the aurora borealis, fluorescence, phosphorescence (afterglow), and chemo- and bioluminescence (firefly, glowworm). Fluorescence is the short-lived emission of light under actinic radiation; it ceases immediately (decay within about 10^{-8} seconds) once the excitation is interrupted. By contrast, phosphorescent matter will continue to glow for some time (decay time 10^{-8} seconds to seconds or even hours) after cessation of the exciting radiation. The practical value of luminescence is that invisible radiation like ultraviolet can be converted into visible light or infrared. Inks, fibers, and planchets based on organic fluorescent substances are frequently used to produce security elements. The luminescence of such elements is absent in white light but is revealed under actinic radiation, commonly a waveband around 365 nm. This is referred to as *longwave ultraviolet*.

Fluorescent compounds can be added to absorbing printing inks as well as to transparent carriers. In the latter case, the fluorescent printing is virtually invisible until irradiated with ultraviolet light. Samples of both types are given in Figure 4.1. Often, bank note numbers and design elements are fluorescent.

A drawback of fluorescent security features is that a multitude of organic luminescent compounds can be commercially obtained or can be synthesized using common optical brighteners. Fraudulent replication would only demand substitution of the authentic material with a luminescent substance that emits light of a similar color. A possibility to overcome this drawback is to apply luminescent materials with unique optical properties that cannot be simulated with commercial materials. Such materials may have proprietary compositions and require high technology for their production. Their inspection often involves machine reading.

An approach is to apply fluorescent security inks that emit different colors in longwave ultraviolet and shortwave ultraviolet wavebands around 365 nm and

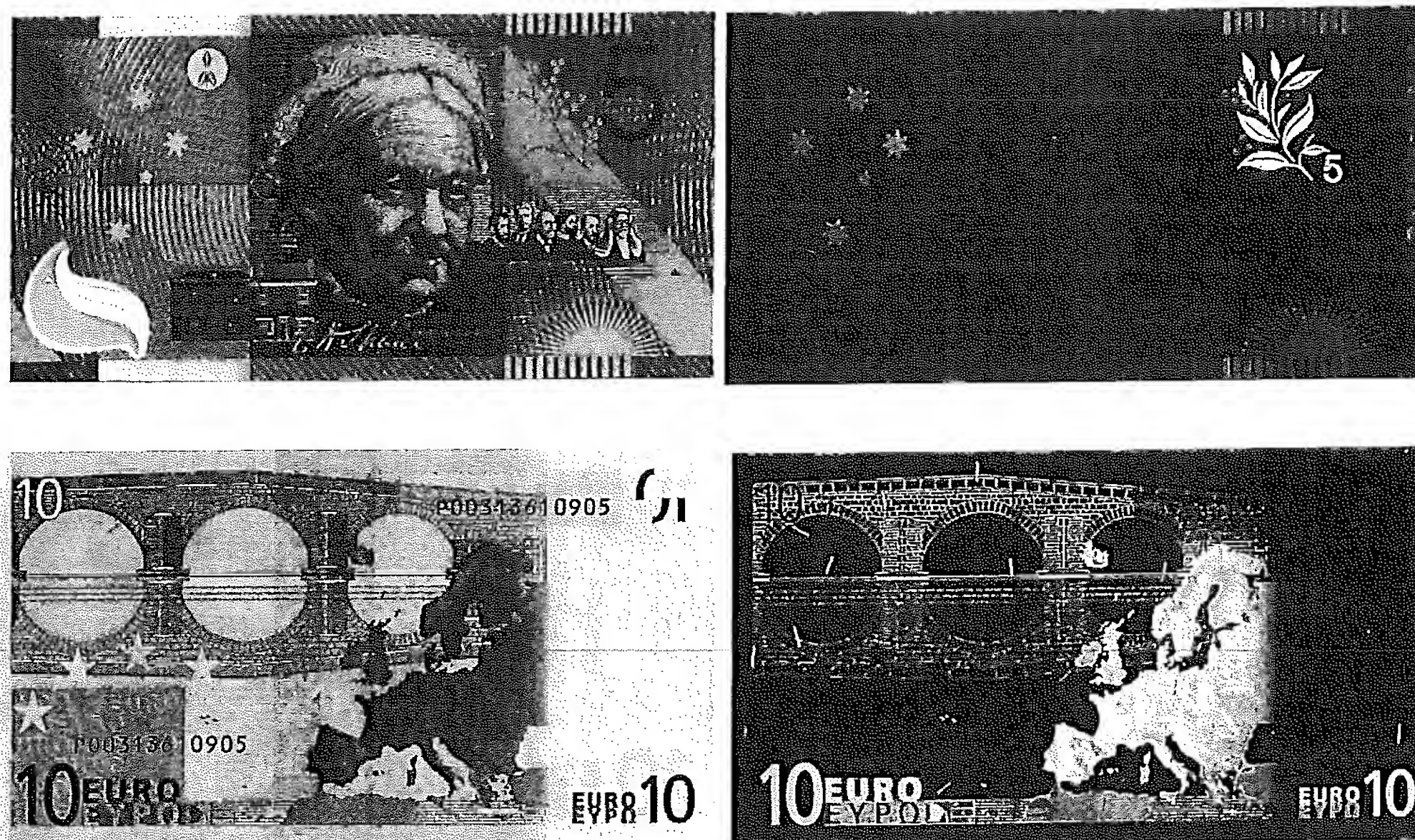


Figure 4.1 Fluorescent printing inks in longwave ultraviolet. Australia \$5 note: Fluorescent absorbing yellow stars and Sun emblem, and leaves in transparent green fluorescent ink (top). €10 note: absorbing brown image elements in yellow fluorescent ink (bottom).

254 nm, respectively. Such inks are only available for established security printers and cannot be easily synthesized. Light sources are available that can be quickly switched between shortwave and longwave ultraviolet irradiation. Examples are given in Figure CD4.2 and Figure 4.2. The fluorescence of other printing inks may be only visible under shortwave ultraviolet illumination, such as the green fluorescent ink in Figure 4.2, or the fluorescence may only be visible under longwave illumination.

The distinction between longwave and shortwave fluorescence sometimes leads to peculiar results in counterfeit bank notes. An example is presented in Figure 4.3. The genuine note in the left column of Figure 4.3 does not show major differences between longwave and shortwave yellow fluorescence of the line offset printing. However, the green and red fluorescence of the note numbers and the fluorescence of the fibers are significantly brighter under longwave illumination. For bank note security, longwave fluorescence is indeed most important because the ultraviolet sources generally in use by cashiers and shopkeepers are longwave-emitting sources.

Surprisingly, particular professional counterfeits of German bank notes show opposite fluorescent characteristics, as shown in the right column of Figure 4.3. Here, the yellow fluorescence of the line offset is virtually absent under longwave illumination. Also, the red fluorescence of the note number is rather faint. Under shortwave illumination, though, a bright yellow fluorescence of the offset printing is present; also, printed security fibers appear, and the note number fluorescence becomes a bright orange. Of course, the efforts taken by

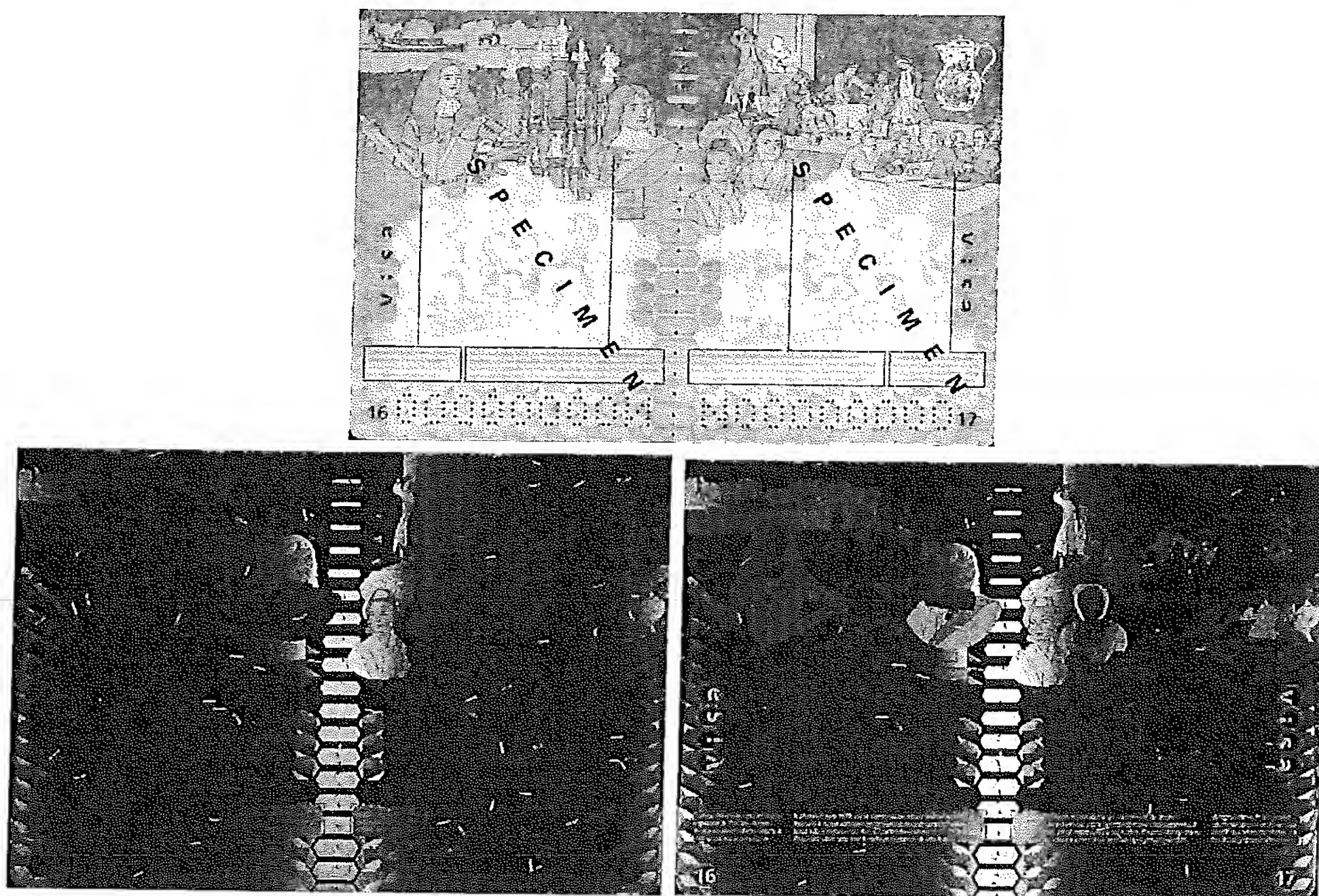


Figure 4.2 Longwave- and shortwave-sensitive fluorescent inks in the 1995 Dutch passport: white light (top); longwave ultraviolet (bottom left); and shortwave ultraviolet (bottom right). All passport pages have different illustrations of Dutch history, narrated in small lettering: cyan in white light and green in shortwave ultraviolet. The illustration shows the pages 16 and 17.

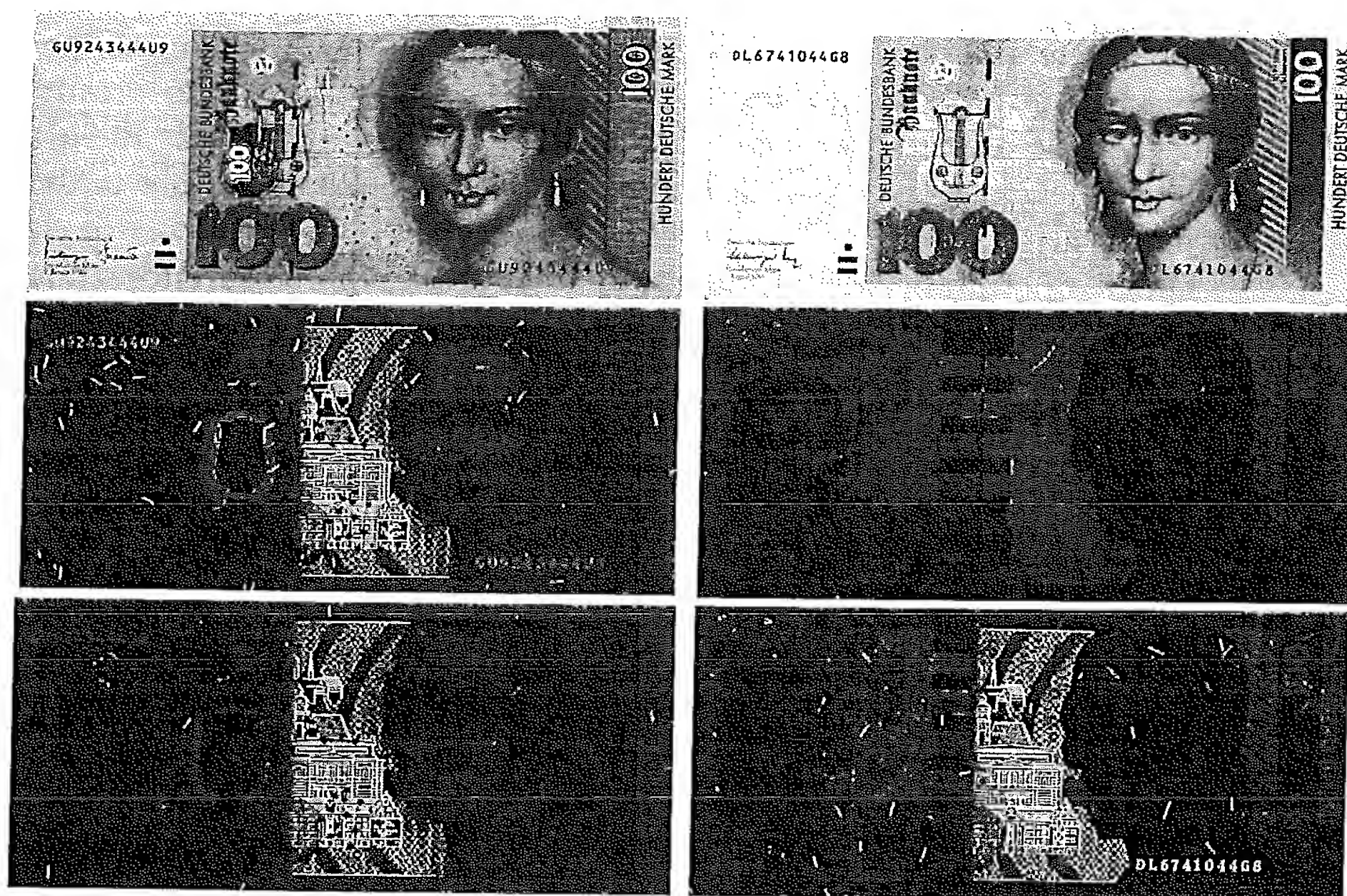


Figure 4.3 Longwave and shortwave fluorescence: genuine German bank note, 1996 issue (left column), and counterfeit German bank note, 1991 issue (right column): white light (top row); longwave ultraviolet (middle row); and shortwave ultraviolet (bottom row).

this counterfeiter are largely useless, because the ultraviolet sources generally in use do not reveal the fluorescence of the printing inks he used. This exemplifies the difficulties that even professional counterfeiters meet in trying to imitate the optical effects of genuine security documents. In general, a wide abyss yawns between the quality of genuine documents and even professional counterfeits. However, distinguishing the counterfeit with the naked eye or with simple equipment requires attention and knowledge of what optical effects must be present. These requirements generally surpass the efforts that the layperson is prepared to take.

Full-color fluorescent images can be created by combining inks that are fluorescent in the three additive primary colors red, green, and blueviolet, as shown in Figure CD4.3. If these inks are transparent, the full-color image is only visible under ultraviolet irradiation and, printed on a transparent security foil, can serve as a security overlay on identification documents.

Normally, fluorescence is emitted in wavebands of longer wavelengths than that of the exciting radiation. Examples were given in Figures 4.1 and 4.2, where ultraviolet excitation resulted in visible fluorescence. Excitation with ultraviolet or visible light may also cause fluorescence in the near infrared, the inspection of which requires machine reading. This type of fluorescence is called Stokes radiation, after Sir George Gabriel Stokes, a nineteenth-century British physicist. However, so-called anti-Stokes compounds, such as certain rare Earth compounds, emit fluorescent radiation of shorter wavelength than that of the exciting source, and these compounds can be added to printable carriers or to the substrate itself. The exciting source may be a small handheld infrared-emitting diode laser ($\lambda = 980$ nm), and the anti-Stokes radiation may be in red, green, or blue visible wavebands, depending on the particular rare Earth applied. Intaglio and screen printing are preferred application methods because these allow the use of relatively large particles of luminescent pigments ($5\text{--}70\text{ }\mu\text{m}$), which is favorable for the luminescence efficiency [5]. Security inks based on antistokes radiation are suitable for first-line inspection with handheld diode lasers, second-line inspection machine reading, and third-line inspection with advanced laboratory equipment to exactly identify the emitted antistokes lines. Security inks can be doped with antistokes pigments in different mutual concentrations, rendering the inks specific spectral responses and thus allowing customization of the inks [6].

Again, another approach is to combine fluorescent and phosphorescent materials in a security element. If the phosphorescent afterglow is short lived, visual discrimination between the two phenomena is impossible. Furthermore, if both materials have similar emission spectra, the presence of two different luminescent substances remains concealed. Short-lived phosphorescence of security inks requires machine detection of the afterglow. A portable phosphorescence detector, which discriminates between fluorescence and short-lived phosphorescence, is described in [7]. It comprises an ultraviolet excitation source, which may be modulated from 25 Hz up to several kilohertz, and a liquid crystal shutter, which is switched between opaque and transparent states in conjunction with the modulation of the excitation source. If the switching is in phase (source on-shutter open, source off-shutter closed), fluorescent and phosphorescent features will both be visible. If, however, the switching is in counterphase (source

on-shutter opaque, source off-shutter open), only phosphorescent features will be visible. Switching the detector between both modes of operation will clearly enable visual or machine discrimination between fluorescence and phosphorescence. Reference is made to Section 9.4.3 of [4] for further details on phosphorescent effects.

4.2.2 Thermochromic Inks

Thermochromic inks reversibly change color with temperature. In security applications, these inks can be inspected in first line by warming to body temperature, at which they become transparent and the color temporarily disappears. The visible color returns once the ink cools to room temperature. The simplest application is to print a design element in thermochromic ink. The element will disappear once warmed by the finger. A more elaborate design uses the thermochromic ink to mask information with an opaque thermochromic ink, whose information will appear once the thermochromic ink is warmed, as shown in Figure 4.4. Another approach is to mask a message in thermochromic ink with a background of common ink in the same color, or vice versa [8]. An example is shown in Figure 4.5.

Thermochromic inks are easily destroyed by excessive heat, and their lightfastness tends to be mediocre at best. This is why thermochromic inks are not used on



Figure 4.4 Thermochromic ink on windowed thread: blue at room temperature masking small text (left), and transparent after warming up between thumb and index finger, revealing small text "sail" (right). (Original image size: 22 × 7 mm.) (Sample courtesy of: DeLaRue, United Kingdom.)

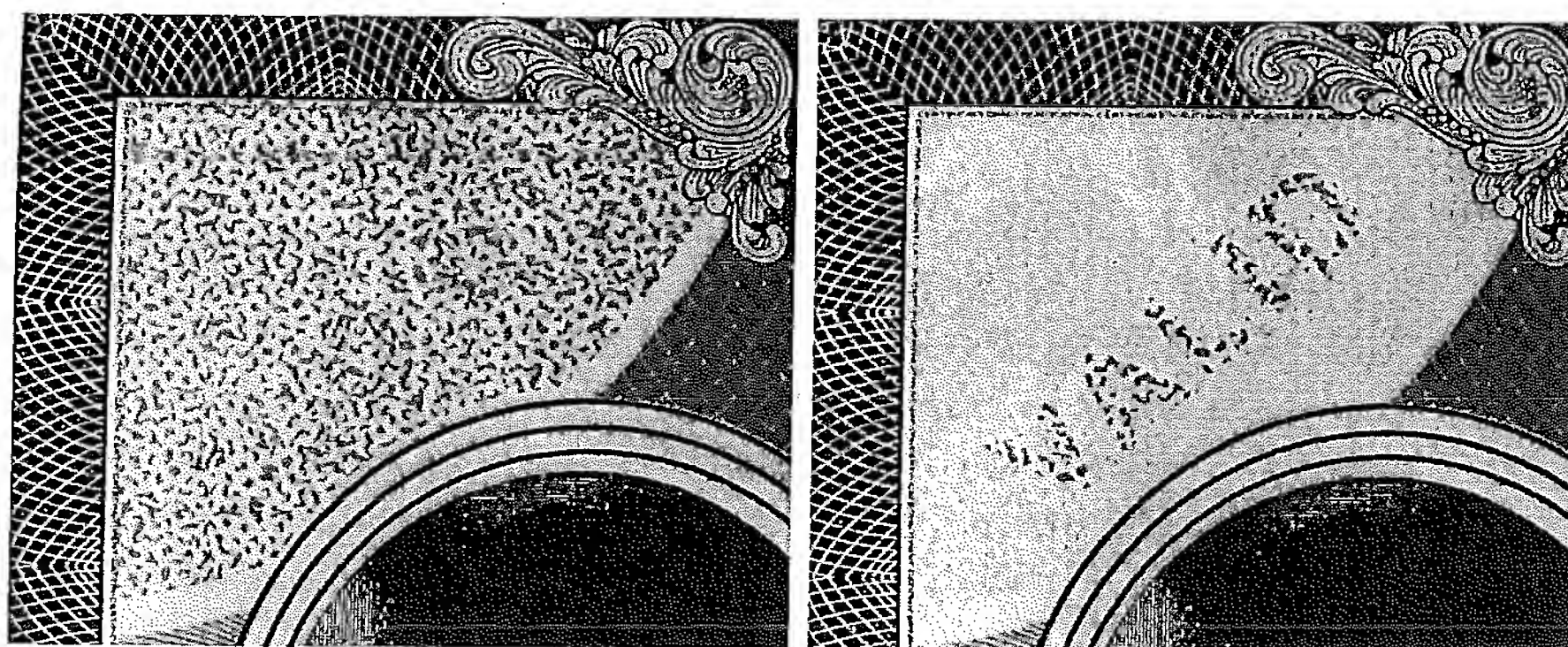


Figure 4.5 A random background printed with thermochromic ink masks the word "valid" printed with common ink of identical color: at room temperature (left), and after warming up to hand temperature (right). (Original image size: 35 × 29 mm.) (Sample courtesy of: CFC Northern Bank Note, United States.)